1. Introduction

Wireless Mobile Ad-Hoc Networks (WMANs) provide more supportive services having the best effort in real-time surveillance due to its prevalence. These networks need to provide Quality of Service in terms of bandwidth, less energy consumption and less delay. In\textsuperscript{1}, discussed about distributing the traffic to save the node energy where it avoids node early expiration due to overload. To do this, load balancing is combined with the energy aware routing mechanism called as Path Efficient and Energy Aware Ad Hoc Multipath Distance Vector (PE-EA-AOMDV) routing protocol. In\textsuperscript{2}, a novel video steganography method is applied by integrating Haar Integer Wavelet Transforms (IWT) and Least Significant Bits (LSB) substitution for hiding the data over RGB channels extracted from video file. This process is carried out on text binary form of the data. Power consumption is reduced by applying a novel power management system where it utilizes a pack of two solar powered batteries and automatic battery switching system. This battery system is used to replace the real time battery used in the node\textsuperscript{3}. But this battery replacement system is used only in certain kinds of applications. In\textsuperscript{4} reported that the link
Wide range of applications are deployed and utilized under WMANs like surveillance monitoring, security sensing in military, home automation, healthcare and traffic monitoring etc. A usual WMAN contains huge number of sensor nodes with a sink node. A sensor node is small in size, having ability to sense and communicate with other sensor nodes in the same/different networks under same frequency remotely. Since the sensor nodes are deployed in remote environments energy becomes the critical issue in WMAN where the sensor nodes are not able to re-charge. Energy becomes a crucial issue because of the dynamic changes in sensor nodes behavior in terms of bandwidth, distance, mobility and so on. The Quality of Service is decreased due to certain problem on top of increasing the throughput of the network in all kind of distributed networks. Amplify-and-Forward method was proposed by for data transmission where the data error, energy consumption among the sender and receiver are rectified and reduced respectively. Whereas the existing energy efficient protocols, mechanisms are not satisfied the user in terms of security. This paper proposed a secured clustering approach where energy efficiency with security is provided by integrating security mechanism and clustering approach together. The security is given in terms of examining nodes, timing and other relevant information collected during data transmission. In the existing research, the author discussed and proposed Defending against DoS (DAD) where DAD works in all the ways to detect and prevent DOS attack. Identity verification, Static IP assignment verification and Auth- key based communication and packet monitoring with time stamp and IP. But WDT-CH approach improves the efficiency of MANET in terms security and improved QoS.

2. Problem Statement

Given a network G is defined as N X N is deployed with M number of nodes randomly. At initial level all nodes energy is assigned to the maximum limit. In the network base station is considered as a sink node or receiver. The entire nodes are deployed in the form of clusters, where each cluster is assigned with a Cluster Head. The Head is also behaved as a timer called “Watch Dog Timer (WDT-CH)-Cluster Head” and it is used to trace the health status of all the nodes deployed in the region specified in specific time called 32 milliseconds. The nodes which are in the path say P will be active throughout the communication. The algorithm runs if ANdD signal of all the nodes in the path should be active. Because of the modes specified node energy is utilized in a very least manner compare to earlier approaches. During sleep mode, no operation is carried out until active or link message to WDT-CH arrives. The message packet which is transmitted from source to sink is encrypted and decrypted and it is controlled by key distribution management. This key distribution is operated by the WDT-CH nodes in the network. The nearest WDT-CH node for the path initially distributes public key to the source and encryption done by providing different key for message packet. The data packet is collected from the source and encryption done in WDT-CH side and transmitted directly to the next hop node where data transmission resumes. By this security is ensured in an esteem level to avoid data leak from the message packet because authorized nodes are participating in the communication and it is monitored by a special monitor node called WDT-CH node.

3. Network Model

A restricted amount of nodes are deployed in the network as cluster wise. Each cluster comprises M number of nodes where M ranges from 1 to 5. Each cluster has minimum of one to maximum of three WDT-CH nodes for improving the security and node status monitoring. Base station is considered as a sink node in which for all paths the sink node is the destination node and it is depicted in Figure 1. Initially all nodes are assigned with Node-ID, initial energy as 100, location (x, y) and cluster-ID. Each Node-ID is clubbed with cluster-ID belongs to the corresponding cluster where the node is placed. Here maximum number of cluster is restricted to 4. Based on this cluster number nodes are identified. At every sample interval each node in the cluster sends its own status word to the selected WDT-CH node. Actually WDT-CH node is considered Main and Redundant. If anyone WDT-CH node fails in the network, spare WDT-CH node will be considered for loop. Hence redundant WDT-CH nodes are kept spare for the cluster in the network. The selected WDT-CH node receives the status word from all the nodes assigned in the cluster and updates the same to base station in case if any node is fault or fails.

Figure 1. Proposed network model.
In the existing clustering approaches the cluster nodes transmit data to CH, the CH transmits the gathered data to BS directly or through other nearest CH to BS.

To ensure the data correctness if any word continuously received from the particular node by stating fail mode for 3 times, then only corresponding node is considered for removal and detach from network. This 3 time check is to ensure the node failure for considerable time. One counter will be run if fail status of node is identified for first time for the corresponding node. If it crossed three then it reset the counter to zero and make that node as a fault node and provide the status to base station stating that not to consider the node for furthermore. The status word is depicted in Figure 2.

The status word transmission is depicted in Figure 3. The status word header format is depicted in Figure 2. The status word is depicted in Figure 2.

Figure 2. WDT-CH Node interaction with sensor nodes.

Figure 3. Status word header format.

Example, consider the bit pattern 11011100 is received by WDT-CHN as an update from node 12 at time t. From this pattern LSB four bits specifies the node-ID, here 1100 called node-ID is 12. And fourth and fifth bit represents the cluster number, here 11 represents node-12 belongs to cluster-2. MSB two bits, it clearly tells that the node is in non-active state of mode, here 11 represents the node-12 is active and 4th bit of the SW.

If apply k = 0, 1, 2 that doesn’t belongs to graph G.

Algorithm:
//Watch dog timer node chk.
//Specification: WDT-CH timer is a network node which keeps track the status word of all the assigned nodes in the cluster for health check in Equal intervals.
//Input: Network G within valid nodes.
//Precondition: All nodes are assigned with a new energy level and authorized by BS.
//Exit criteria: All assigned nodes health check receive 0.
//Post Condition: Active status of WDT-CH node in clustered network.
//exit Criteria: Path P found. Path_Routing TREE, Begin.

Algorithm-2: Path_Routing_Tree
// input: Network G with {v} authorized nodes, Clustered node deployment by Sink node.
//Precondition: Active status of WDT-CH node in clustered network.
//exit Criteria: Path P found. Path_Routing_TREE, Begin.

Algorithm-1: WDT-CH chk_node ( )
Begin:

Theorem-1:
Let ‘G’ be a regular graph. Then there exists a sub graph ‘G’ which depends on ‘G’. Such that every node ‘u’ in ‘G’ such ||W|| ≥ G, we can break u in to:

• for all \( i \geq 0 \), the graph node \( \alpha G^\infty \) is also in graph G.

Example, consider the bit pattern 11011100 is received by WDT-CHN as an update from node 12 at time t. From this pattern LSB four bits specifies the node-ID, here 1100 called node-ID is 12. And fourth and fifth bit represents the cluster number, here 11 represents node-12 belongs to cluster-2. MSB two bits, it clearly tells that the node is in non-active state of mode, here 11 represents the node-12 is active and 4th bit of the SW.

iv. At time \( T_i \) \( T_{i+1} \)...
WDT-CH and (WDTCH1, ..., WDTCHn) Node and timer specifies how node is transmitting the status word to it.
call Active;
end loop
return (Ti < Pi)
end Path, Routing, Tree

• Algorithm-3: Data Packet Transmission
// Input: 1. Path P 2. Constructed routing tree for path P
// Output: 1. Path P and Tree Ti is set
// Exit Criteria: If data packet received by sink or Transmission called off.
Data_pkt, Tx_SrcToSink.

Begin
node< Pi
next_hop Pi+1
{ Clusterc, Clusterp---Cluster e P } < WDT-
CH-LooP ClusteRi...Cluster e P then
WDT-CH<-nextHop(Cluster)
(Cluster_c P ) < WDT-CH
Data <- encryption_pkt[Data]
(Node (Cluster e P ) ) < Data
if node state fails
WDT-CH<- n(-1)
next_hop <- P,
WDT-CH<-SinkNode(Data)
node(n).data <- WDT-CH
end if
else clear data pkt from WDT-CH
Path <- 0
WDT-CHf <- Primitive
RoutingTreef< 0
endData_pkt, Tx_SrcToSink

The above algorithm has three partitions called steps, they are:
• Watch Dog Timer Based Node Check.
• Path Routing Tree.
• Secured Data Transmission.

WDT-CH based node check is a network node which keeps track the status word of all the assigned nodes in each cluster to derive the health check. There is main and redundant WDT-CH nodes are identified in each cluster to monitor the other sensor nodes in the region. The same is described in Algorithm 1. Consider the network with randomly deployed nodes maximum 4 clusters it will be partitioned. Each sub clusters is organized by WDT-
CH node. At specific time intervals all the nodes in the cluster transferred the status word packet to the selected WDT-CH node for loop. From the status word state of the node is derived with health check and the same is passed to the base station. BS keeps trace of node by status word specification. Status table is maintained if any node information in future requires about the nodes the recent status word details is in this status table. It ensures the recent health check of the nodes participated in the network. If health check is affirmative then the nodes are in good condition to support data communication, whereas if health check is not affirmative then from WDT-CH side one counter is assigned to ensure the same health check for 3 time, after 3 count the same status remains from the node, then the node which health is not affirmative is removed from the network. The same is intimated to BS. For future communication or path discovery the node will not be considered.

In path routing tree, the path nodes are connected without ambiguity to the destined node. A path which is considered for communication is done after the collective AND check of all the nodes in the path. Active flag is used in software side reads the active status from the sensor nodes in the path. If this flag is set then based on the route, routing table is updated with next hop nodes. The same step is followed until all the nodes in the path are considered for routing table update. Finally routing tree is formed based on the valid path and ready for transmission.

Data transmission is starts from the source node by holding the data packet and passed to the authorized node in the path by routing table next hop. Here key distribution scheme is handled by WDT-CH node. Initially WDT-CH node will send key to path nodes for ensuring the communication. Based on the next hop the current node knows the next node and request WDT-CH to pass the data packet to next node. WDT-CH is now assigns two keys one to current node and one to target node. With that encryption happens in current node, the key which sent to target node is used for accepting the data packet. It will not decrypt to identify data, here for acceptance of data packet key is used, the general data is encrypted in initial node. Individual encryption and decryption is to check whether valid nodes in the path are used for communication. With the help of WDT-CH node key is received by both the ends of data transmission tag. If decryption fails or any failures like data packet loss during transmission, WDT-CH node declares transmission failure. This WDT-CH node knows the tag nodes will use the key in the stipulated time. If no key requirement triggered from tag end, it declares the failure. In this case, WDT-CH node receives the data packet from the source node and delivers to next hop node where data transmission paused. Then continuity of process is same like proposed method until sink receives the data. After successful completion of data transmission path is cleared and tree is available for next dynamic update.

3.1 Routing Tree

An unambiguous tree structure is formed by linking path nodes from source to sink node which is called BS. Parent child links is established for packets forward. High efficient bandwidth and energy is utilized for data communication. A node receives the data packet based on the next hop link and in the order of tree structure, a set of protocols and rules are certain to the MAC cluster node, with the help of WDT-CH node it passes to the other node in an efficient way by secured encryption methods. The tree structure is depicted in Figure 5. The path metrics in the tree obtained is calculated by as follows:

Path Metric in routing tree:

\[ M_{p} = \frac{\text{No of Hops For Path}}{\text{Max (load in path)}} \times \text{Probability of PATH Success} \]

• The structure consists of flow control mechanism which acknowledges for every node communication. The proposed approach is comparatively studied with earlier approaches like secured energy efficient mechanism.

5. Results and Discussion

The simulation network taken considerable nodes to pass the algorithm, based on the output the basic metrics like throughput, Packet Delivery Ratio (PDR), End-End Delay. Residual energy is calculated and the same is compared with earlier approach. Time with delay is compared and shown in Figure 6. Time is considered in seconds and delay is verified with the data transmit of packets from source and receiver of each node. End of iteration the node communication is estimated with transmission time and node delay. In existing approach delay obtained is maximum level where time increases. Using WDT-CH nodes here the delay is qualified in transmission stage from one node to the other. If node fails to trigger for data transmission within the stipulated time, WDT-CH will take care of further process, hence delay is handled optimistic.
Figure 7 depicts the comparison of Packet Delivery Ratio between existing and proposed approach. Number of nodes considered here in terms of 10 to 70, each time the probability of successive PDR obtained is calculated as follows:

\[
PDR = \frac{\text{# PacketsReceived}}{\text{# PacketsTransmitted}}
\]

For the approximate time within the specified range, how many packets are received by the sink node is given in the Figure 7. It clearly states that for proposed approach PDR is high that is for maximum number of packets transmitted, all packets which is controlled by WDT-CH node is received by the sink node.

In this proposed approach, main goal is how to use energy efficiently when sensor node really not in use. For this several nodes is identified in proposed system, each node usage and activities is clearly handles the anomalies in energy efficiency. It is depicted in Figure 8, number of nodes is compared with energy levels. Node is considered in all cluster levels as per the network model. All nodes are in different modes, mostly in sleep mode except path nodes in action or node busy in sending status word. This approach is compared with existing system; the proposed model defines efficient energy usage between the nodes.

Since this proposed approach follows clustering technique, the efficacy of the energy saving is verified in the simulation. To do this, the simulation is carried out five rounds where in each round the number of nodes deployed is varied. In all the five rounds there are 200 number of nodes in increased from round one to round five. After each round the remaining energy of the cluster nodes are calculated and verified. According to the data size, distance among the nodes and the Cluster Head, clusters in the network also increases. Hence, WDT-CH shall be selected based on centric access to energy level in the network. By this proposed model, energy level decreases, clusters in the network also increases. Hence, WDT-CH shall be selected based on centric access to energy level in the network. In future, if the status word size increases, network size also increase with more number of nodes. Over to this, WDT-CH node for each cluster main and redundant is used here, if any one WDT-CH sensor node fails, the other one is considered for a loop. If number of nodes increases, clusters in the network also increases. Hence, WDT-CH shall be selected based on centric access to energy level in the network.

6. Conclusion

The main objective of the paper is to reduce the energy consumption among the nodes and improving the security. To do this WDT-CH node based monitoring the nodes health status to communicate efficiently. Here, WDT-CH node is acting as a Cluster Head as well as monitoring node in the clusters and since it is efficient to provide security and energy efficient in the network. This secured clustering leads to prevent data loss and reduce the delay while routing. From the simulation results it is clear and concluded that the proposed WDT-CH approach is efficient mechanism for improving secured energy efficient network. In future, if the status word size increases, network size also increase with more number of nodes. Over to this, WDT-CH node for each cluster main and redundant is used here, if any one WDT-CH sensor node fails, the other one is considered for a loop. If number of nodes increases, clusters in the network also increases. Hence, WDT-CH shall be selected based on centric access to the cluster nodes. By this proposed model, energy level is consumed up to the maximum consumption using different mode specified and security is implemented throughout the communication.

7. References

